Gouvernement du Canada | Government of Canada

RAPPORT D'ÉTAPE SUR LES

ÉVOLUTIONS EN MATIÈRE DE LÉGISLATION SUR LA PROTECTION DES DONNÉES AU CANADA (2001-2017)

Rapport à la Commission européenne mai 2017

Canada

Cette publication est également offerte en ligne : http://www.ic.gc.ca/eic/site/iccat.nsf/fra/07392.html.

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication : www.ic.gc.ca/demande-publication ou communiquer avec :

Centre de services Web
Innovation, Sciences et Développement économique Canada

Édifice C.D.-Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5
Canada

Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
TTY (pour les personnes malentendantes) : 1-866-694-8389
Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)
Courriel : ISDE@Canada.ca

Autorisation de reproduction

À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission du ministère de l'Industrie, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, que le ministère de l'Industrie soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec le ministère de l'Industrie ou avec son consentement.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, veuillez demander l'affranchissement du droit d'auteur de la Couronne : www.ic.gc.ca/demande-droitdauteur ou communiquer avec le Centre de services Web aux coordonnées ci-dessus.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de l'Industrie, (insérer l'année de publication).

N° de catalogue Iu37-8/2018F-PDF
ISBN 978-0-660-25849-2

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

Also available in English under the title *Update Report on Developments in Data Protection Law in Canada (2001-2017)*

Table des matières

1.0 Introduction 4

2.0 Le contexte canadien 4

3.0 Loi canadienne régissant la protection des renseignements personnels dans le secteur privé (*Loi sur la protection des renseignements personnels et les documents électroniques*) 6

4.0 Loi canadienne régissant la protection des renseignements personnels dans le secteur public (*Loi sur la protection des renseignements personnels*) 10

5.0 *Charte canadienne des droits et libertés* 12

6.0 Accès à des fins d'application de la loi et de sécurité nationale 13

7.0 Évolutions récentes 17

8.0 Renseignements complémentaires et rapports 19

1. 0 Introduction

1.1. Le 20 décembre 2001, la Commission européenne (CE) rendait la Décision 2002/2/CE, dans laquelle il est dit qu'aux fins du paragraphe 6 de l'article 25 de la Directive 95/46/CE (ci-après appelée la « Directive »), le Canada est considéré comme assurant un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne (UE) aux destinataires assujettis à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

1.2. Cette décision permet aux exploitants de l'UE d'envoyer au Canada certaines données à caractère personnel à des destinataires assujettis à la LPRPDE sans qu'il leur faille prendre des mesures de protection additionnelles pour répondre aux exigences de la Directive.

1.3. Dans la Décision d'exécution (UE) 2016/2295 du 16 décembre 2016, la CE modifiait la Décision 2002/2/CE pour se conformer à l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems contre Data Protection Commissioner.

1.4. Conformément à l'article 2 de la Décision d'exécution (UE) 2016/2295, la CE est maintenant tenue de suivre, de manière permanente, les évolutions de l'ordre juridique canadien, notamment les évolutions concernant l'accès des autorités publiques aux données à caractère personnel, afin d'évaluer si le Canada continue d'assurer un niveau de protection adéquat des données à caractère personnel.

1.5. Dans une lettre datée du 25 janvier 2017, la Direction générale de la justice et des consommateurs de la CE invitait le Canada à aider la Commission à s'acquitter de ses obligations de surveillance en lui fournissant de l'information sur toute modification ou évolution importante intervenue depuis la Décision 2002/2/CE en matière de protection de la vie privée et des données. La correspondance demandait également de l'information sur les limitations et les mesures de protection entourant l'accès des autorités publiques canadiennes aux données à caractère personnel, en particulier à des fins d'application de la loi et de sécurité nationale.

1.6. Afin d'aider la Commission à respecter ses obligations de surveillance en vertu de la Décision d'exécution (UE) 2016/2295, le présent rapport provisoire présente :

- les évolutions intervenues dans le cadre canadien de protection des données s'appliquant aux organisations du secteur privé et aux entités gouvernementales;
- l'information sur les limitations et les mesures de protection régissant l'accès des autorités publiques aux données à caractère personnel, en particulier à des fins de sécurité nationale et d'application de la loi.

2.0 Le contexte canadien

2.1 Au Canada, la *Charte canadienne des droits et libertés* (la « *Charte* ») est une loi fondamentale garantissant la protection des droits de la personne en vertu de la Constitution. Cela comprend le droit à la vie, à la liberté et à la sécurité de sa personne en vertu de l'article 7, le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives en vertu de l'article 8 et l'égalité devant la loi en vertu de l'article 15. Toutes les lois et mesures gouvernementales d'ordre fédéral et provincial doivent se conformer à la *Charte*, que les tribunaux peuvent faire

respecter. Intégrée dans la Constitution du Canada, la *Charte* prévaut sur les autres lois et définit les limites de l'action gouvernementale.

2.2 Au niveau fédéral, le cadre de protection de la vie privée du Canada repose sur deux lois centrales en la matière. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[1] constitue l'assise juridique pour le secteur privé, en établissant la manière dont les entreprises doivent protéger et gérer les renseignements personnels dans le cadre d'activités commerciales. La *Loi sur la protection des renseignements personnels* constitue l'assise juridique pour la collecte, la conservation, l'utilisation et la communication de renseignements personnels par les institutions gouvernementales qui lui sont assujetties.

2.3 Toute activité gouvernementale, qu'elle soit autorisée par la loi ou la common law, est assujettie aux restrictions de la *Charte*. En outre, le traitement des renseignements personnels par le gouvernement obéit toujours à un cadre de lois du secteur public. Certaines de ces lois confèrent au gouvernement des pouvoirs spécifiques lui permettant de recueillir, d'utiliser, de conserver ou de communiquer des renseignements personnels à des fins particulières.

2.4 De la magistrature indépendante émane la jurisprudence servant à interpréter les pouvoirs publics et les droits civils. Les particuliers ont accès à des mécanismes de surveillance spécialisés tels que le Commissariat à la protection de la vie privée du Canada et le Bureau du vérificateur général du Canada, ainsi qu'à plusieurs organes chargés d'examiner les activités des principaux organismes de sécurité nationale (p. ex. le Comité de surveillance des activités de renseignement de sécurité et la Commission civile d'examen et de traitement des plaintes relatives à la Gendarmerie royale du Canada).

2.5 Les ministères sont tenus d'exercer les pouvoirs qui leur sont conférés par la loi dans le respect des politiques et des lignes directrices établies par le président du Conseil du Trésor, en sa qualité de ministre responsable, et, le cas échéant, de tout règlement promulgué en vertu d'une loi.

2.6 Dans le système juridique canadien, les décisions des tribunaux en matière de droit public sont considérées comme des précédents contraignants auxquels doit obéir toute instance judiciaire future et tout fonctionnaire chargé d'appliquer la loi. Il s'ensuit qu'au fil du temps, les tribunaux formulent des interprétations souvent plus restrictives des lois que ne le donnerait à penser le libellé en apparence plus général de celles-ci. Ces interprétations sont influencées tant par le principe de common law selon lequel les lois ayant pour effet de restreindre les droits ont tendance à être interprétées restrictivement que par celui selon lequel cette interprétation devrait être guidée par la *Charte*. Pour déterminer l'effet réel d'une disposition donnée, il faut, par conséquent, lire la législation canadienne parallèlement à la jurisprudence applicable.

2.7 En résumé, le Canada dispose à la fois d'un cadre de protection des données régissant le secteur privé et d'un tel cadre régissant le secteur public, que l'on comprendra mieux sachant que, dans système juridique canadien, les activités du gouvernement sont assujetties à la primauté du droit, aux exigences de la raisonnabilité, au respect de limites réglementaires équilibrées, aux institutions de surveillance et à des mécanismes internes de conformité.

[1] Les lois fédérales canadiennes se trouvent à http://laws.justice.gc.ca/fra/.

3.0 Loi canadienne régissant la protection des renseignements personnels dans le secteur privé (*LPRPDE)*

3.1 La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), la loi fédérale du Canada protégeant la vie privée et les données dans le secteur privé, établit l'équivalence juridique pour les documents électroniques. Sa partie 1 fixe les règles juridiques régissant la protection des renseignements personnels au Canada. La LPRPDE s'applique à toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales. Elle ne s'applique ni aux organisations du secteur public, qui sont régies par la *Loi sur la protection des renseignements personnels*, ni aux organisations régies par le secteur public à l'échelle provinciale. La LPRPDE fixe des limites à la collecte, à l'utilisation et à la communication de renseignements personnels par les organisations. Elle établit également les circonstances restreintes et précises dans le cadre desquelles les organisations communiquent des renseignements personnels aux institutions gouvernementales et aux organismes d'application de la loi. L'application de la LPRPDE se fonde sur le modèle de l'ombudsman, les mécanismes de surveillance et de recours relevant du Commissariat à la protection de la vie privée du Canada (CVPC) et de la Cour fédérale. En sa qualité d'organisme fédéral chargé de la protection des données, le CVPC a pour mission de protéger et de promouvoir le droit des personnes à la vie privée.

3.2 La LPRPDE, entrée en vigueur le 1er janvier 2001, est un régime avancé et hautement respecté de protection de la vie privée. Elle assure un équilibre entre le droit à la vie privée des individus et le besoin légitime des entreprises de recueillir, d'utiliser ou de communiquer des renseignements à des fins raisonnables. Elle se fonde sur une série de dix principes de la vie privée[2] qui ont résisté à l'épreuve du temps. À l'instar des lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) en matière de vie privée[3], qui lui ont servi de fondement, la LPRPDE est un cadre s'articulant autour de principes qui est demeuré intact; seules quelques retouches législatives bien précises y ont été apportées pour en améliorer l'efficacité.

Essentiellement similaires

3.3 Afin de faciliter l'élaboration de lois fédérales et provinciales harmonisées sur la protection de la vie privée, une disposition de la LPRPDE permet à des lois provinciales d'être considérées comme étant « essentiellement similaires » en vertu de celle-ci. Au terme d'un processus formel visant à le déterminer, sont dites essentiellement similaires les lois « qui fournissent un mécanisme de protection des renseignements personnels conforme et équivalent à celui de la LPRPDE, intègrent les dix principes de l'annexe 1 de la LPRPDE, fournissent un mécanisme indépendant et efficace de surveillance et de recours ainsi que des pouvoirs d'enquête et restreignent la collecte, l'utilisation et la communication des renseignements personnels à des fins appropriées et légitimes ».

3.4 Les provinces qui ont de telles lois sont exemptées de la LPRPDE, ce qui leur permet d'assujettir la collecte, l'utilisation ou la communication de renseignements personnels à leurs propres lois. La LPRPDE continue toutefois de s'appliquer à la collecte, à l'utilisation ou à la communication de renseignements personnels relativement à des entreprises fédérales dans la province en question, ainsi qu'à la collecte, à l'utilisation ou à la communication de renseignements personnels à l'extérieur de celle-ci. Plusieurs lois provinciales ont reçu la désignation « essentiellement

[2] Les dix principes énoncés à l'annexe 1 de la LPRPDE sont : la responsabilité, la détermination des fins de la collecte des renseignements, le consentement, la limitation de la collecte, la limitation de l'utilisation, de la communication et de la conservation, l'exactitude, les mesures de sécurité, la transparence, l'accès aux renseignements personnels et la possibilité de porter plainte à l'égard du non-respect des principes.

[3] Lignes directrices de l'OCDE en matière de vie privée, 2013 : https://www.oecd.org/fr/sti/ieconomie/privacy-guidelines.htm.

similaire »; elles s'appliquent de manière générale à des fonds de renseignements personnels d'organisations œuvrant dans la province ou de manière exclusive à des renseignements personnels sur la santé.

3.5 Le Québec, l'Alberta et la Colombie-Britannique ont adopté leurs propres lois de protection des renseignements personnels dans le secteur privé. Celle du Québec a été jugée essentiellement similaire à la LPRPDE en 2003, tandis que celles de l'Alberta et de la Colombie-Britannique l'ont été en 2004. Des lois sur la protection des renseignements personnels dans le secteur de la santé ont été promulguées en Ontario, au Nouveau-Brunswick, à Terre-Neuve-et-Labrador et en Nouvelle-Écosse et ont été jugées essentiellement similaires en 2005, en 2011, en 2012 et en 2016 respectivement.

Examen législatif de la LPRPDE

3.6 Un comité parlementaire doit effectuer un examen législatif de la LPRPDE tous les cinq ans. Le premier examen législatif de la LPRPDE a mené, en 2015, à l'adoption de la *Loi sur la protection des renseignements personnels numériques*. Bien que le projet de loi ait reçu la sanction royale le 18 juin 2015, le nouveau régime de signalement obligatoire des atteintes à la protection des données, qui forme la section 1.1 de la LPRPDE, entrera en vigueur dès que le règlement régissant les incidents d'atteinte à la protection des données sera définitif.

***Loi sur la protection des renseignements personnels numériques* (2015)**

3.7 La *Loi sur la protection des renseignements personnels numériques* (2015) a modifié la LPRPDE de trois manières importantes par l'ajout :

- de mesures pour protéger les consommateurs;
- de dispositions liées aux exceptions concernant le consentement;
- de mesures d'accroissement de la conformité.

Protéger les consommateurs

3.8 *Nouvelle section 1.1 sur la notification des atteintes à la protection des données :* Au nombre des modifications apportées en 2015 à la LPRPDE figure une nouvelle section intitulée « Atteintes aux mesures de sécurité », qui fait état des exigences de signalement par les organisations de toute violation aux renseignements personnels découlant d'une atteinte aux mesures de sécurité présentant un « risque réel de préjudice grave à l'endroit de l'intéressé ». Les organisations devront déclarer toute atteinte aux mesures de sécurité ayant trait à des renseignements personnels au commissaire à la protection de la vie privée du Canada et en aviser les personnes touchées. Ces changements donneront davantage de pouvoirs aux consommateurs et encourageront les entreprises à se doter de meilleures pratiques de sécurité de l'information.

3.9 *Tenue d'un registre des atteintes à la protection des données :* Les organisations devront tenir et conserver un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elles ont la gestion et donner accès au registre sur demande au commissaire à la protection de la vie privée. Celui-ci pourra ainsi remplir le mandat de surveillance qui lui incombe et veiller à ce que les organisations déclarent les atteintes susceptibles d'entraîner un préjudice.

3.10 *Consentement amélioré :* De nouvelles exigences entourant l'obtention du consentement à la collecte, à l'utilisation ou à la communication de renseignements personnels ont été adoptées afin de protéger les personnes

vulnérables, en particulier les enfants. Elles veillent à ce que les organisations souhaitant recueillir des renseignements personnels en communiquent clairement et intelligiblement le but aux utilisateurs cibles.

Exceptions au consentement

3.11 *Intérêt public :* De nouvelles dispositions ont été ajoutées afin de rendre plus claires les situations où, pour des raisons d'intérêt public, les organisations sont autorisées à communiquer des renseignements personnels à l'insu ou sans le consentement de l'intéressé, ces situations sont les suivantes : i) identifier un individu qui est blessé, malade ou décédé, et communiquer avec son parent le plus proche; ii) prévenir une fraude, la détecter ou y mettre fin; et iii) protéger la victime d'exploitation financière.

3.12 *Échange de renseignements :* Des modifications ont été apportées à l'article 7 de la Loi en ce qui a trait à la communication entre organisations de renseignements personnels à l'insu de l'intéressé ou sans son consentement. Auparavant, l'échange d'information entre organisations relevait d'un régime d'organismes d'enquête en application duquel les organisations ainsi désignées en vertu de la Loi pouvaient communiquer des renseignements personnels à d'autres organismes d'enquête. Ce régime a été abrogé et remplacé par les circonstances particulières justifiant l'échange de renseignements, en l'occurrence pour enquêter sur la violation d'un accord ou une infraction à une loi ou pour détecter une fraude, y mettre fin ou la prévenir.

3.13 *Activités commerciales à des fins particulières :* De nouvelles dispositions précisent qu'il est interdit aux organisations de recueillir, d'utiliser et de communiquer des renseignements personnels à l'insu de l'intéressé ou sans son consentement à moins qu'ils ne soient nécessaires à la conduite d'activités commerciales spécifiques et légitimes. Cela comprend les renseignements :

- qui sont produits par l'intéressé dans le cadre de son emploi, de son entreprise ou de sa profession (produit du travail);
- qui ont trait à une transaction commerciale telle qu'une acquisition, qu'elle soit éventuelle ou déjà effectuée;
- dont ces organisations ont besoin pour établir ou gérer la relation d'emploi avec l'intéressé ou pour y mettre fin;
- qui sont contenus dans la déclaration d'un témoin relative à une réclamation d'assurance.

Conformité accrue

3.14 *Nouveaux accords de conformité* : L'article 17.1 de la LPRPDE comporte de nouvelles dispositions permettant au Commissariat à la protection de la vie privée de conclure avec une organisation un accord de conformité visant à faire respecter la Loi. Ce nouvel outil réglementaire offre d'autres recours que les tribunaux ou les sanctions lorsqu'une organisation est reconnue avoir contrevenu à une obligation en vertu de la Loi. Ces accords permettent aux organisations de prendre l'engagement contraignant d'agir pour se conformer à la Loi et leur évitent de coûteuses poursuites en justice. Elles permettent parallèlement au commissaire de tenir les organisations responsables lorsqu'elles manquent à leur obligation de protéger leurs clients.

3.15 *Délai accru pour présenter une demande d'audience :* De nouvelles dispositions prolongent le délai dont jouit un plaignant pour présenter une demande d'audience à la Cour fédérale du Canada. Les parties plaignantes, y compris le commissaire, disposent d'une année au terme d'une enquête pour demander à la Cour fédérale d'ordonner à une

organisation de se conformer à la loi ou d'accorder des dommages à un individu lésé par une atteinte à sa vie privée. Cela donne à l'organisation davantage de temps pour prendre volontairement des mesures de redressement ou négocier un accord de conformité.

3.16 *Amendes et pénalités additionnelles :* De nouvelles infractions ont été créées pour avoir sciemment omis de déclarer une atteinte à la protection des données au commissaire ou d'en informer un individu ou pour avoir délibérément omis de garder ou sciemment détruit des dossiers sur de telles atteintes. Les organisations contrevenantes sont passibles d'une amende pouvant atteindre 10 000 $ par procédure sommaire et 100 000 $ par mise en accusation.

Autres évolutions

3.17 *Ajout de l'annexe 4 :* La LPRPDE a été modifiée en 2015 pour y préciser qu'elle s'applique à l'Agence mondiale anti-dopage (AMA)[4]. Le paragraphe 4(1.1) de même qu'une nouvelle annexe (annexe 4) ont été ajoutés à la LPRPDE afin d'y inscrire l'AMA et d'autres organisations.

Modifications corrélatives à la LPRPDE

3.18 La LPRPDE a été modifiée quatre fois par suite d'autres initiatives législatives au Canada. L'adoption de la *Loi canadienne anti-pourriel* en 2014, le renforcement de la *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles* en 2005, les modifications à la *Loi sur la sécurité publique* en 2004 et l'adoption de la *Loi antiterroriste*, qui est entrée en vigueur en décembre 2001, ont toutes modifié corrélativement la LPRPDE. Les quatre modifications législatives sont décrites ci-dessous.

3.19 La *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique*, plus communément appelée *Loi canadienne anti-pourriel* (LCAP), est entrée en vigueur le 1er juillet 2014. À ses modifications corrélatives à l'article 7 de la LPRPDE visant à introduire de nouvelles définitions liées aux adresses électroniques s'ajoutaient plusieurs nouvelles dispositions relatives aux contraventions, aux nouveaux pouvoirs discrétionnaires du commissaire à la protection de la vie privée, aux pouvoirs de celui-ci de travailler en coordination avec les commissaires des provinces et territoires et à l'échange d'information au sujet d'enquêtes avec des homologues étrangers.

3.20 En novembre 2005 entrait en vigueur la *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*, qui comportait des modifications corrélatives à la LPRPDE. L'article 57, notamment, modifie l'article 9(3) de la LPRPDE et sert à protéger l'identité des dénonciateurs. De plus, une exception discrétionnaire a été ajoutée à la LPRPDE pour refuser de divulguer des renseignements personnels après le dépôt d'une demande officielle d'accès. La modification a été ajoutée « de façon à renforcer davantage la protection de l'identité des parties aux divulgations d'actes répréhensibles au sein des organisations ».

3.21 La *Loi modifiant certaines lois fédérales et édictant des mesures de mise en œuvre de la convention sur les armes biologiques ou à toxines, en vue de renforcer la sécurité publique*, plus communément appelée *Loi de 2002 sur la sécurité publique*, est entrée en vigueur le 6 mai 2004. L'article 7 de la LPRPDE a été modifié afin de permettre la collecte et l'utilisation de renseignements personnels pour des motifs de sécurité nationale, la défense du Canada ou la

[4] L'AMA est une organisation internationale dont le siège social est situé au Canada (à Montréal) et qui a pour mission de promouvoir, de coordonner et de superviser la lutte contre l'usage illicite de drogues dans le sport.

conduite des affaires internationales ou lorsque la communication de ces renseignements est exigée par la loi. La modification précisait que les organisations assujetties à la LPRPDE ont le pouvoir de recueillir et d'utiliser des renseignements au sujet d'individus à l'insu ou sans le consentement de ceux-ci en vue d'une telle communication. L'article 7 de la LPRPDE a fait l'objet d'une modification subséquente en vertu de la *Loi sur la protection des renseignements personnels numériques* de 2015 susmentionnée.

3.22 La *Loi antiterroriste* est entrée en vigueur le 18 décembre 2001. Des modifications corrélatives ont été apportées aux paragraphes 7(3) et 9(2.3) de la LPRPDE afférents à la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*. La LPRPDE a de nouveau été modifiée pour l'harmoniser aux dispositions de la *Loi sur la preuve au Canada* concernant la transparence et l'accès des individus à leurs renseignements personnels et pour assurer « l'équilibre judiciaire entre l'intérêt du public à l'endroit de la communication et l'intérêt de l'État à l'égard de la sécurité nationale et la conservation des renseignements obtenus à titre confidentiel d'une entité étrangère ».

4.0 Loi canadienne régissant la protection des renseignements personnels dans le secteur public (*Loi sur la protection des renseignements personnels*)

4.1 La *Loi sur la protection des renseignements personnels* s'applique à tous les ministères et à la plupart des organismes du gouvernement fédéral de même qu'aux sociétés d'État et à leurs filiales à cent pour cent. Elle limite la collecte de renseignements personnels par les institutions gouvernementales à ceux liés directement à leurs programmes ou activités. La Loi exige des institutions gouvernementales qu'elles recueillent des renseignements personnels à des fins administratives directement auprès des individus autant que possible et qu'elles informent ceux-ci de l'objet de cette collecte. Elle exige également de ces institutions qu'elles utilisent les renseignements personnels aux fins auxquelles ils ont été recueillis, pour les usages qui sont compatibles avec ces fins, avec le consentement de l'individu à qui ils se rapportent ou pour les fins auxquelles ils peuvent être communiqués en vertu de la Loi.

4.2 La Loi permet aux institutions gouvernementales de communiquer des renseignements personnels avec le consentement de l'individu concerné ou sous réserve d'un ensemble restreint de permissions de divulgation, qu'elle énonce. Elle fixe les règles de conservation et de retrait après usage de certains renseignements personnels auxquelles les institutions gouvernementales doivent se conformer. Elle donne aux citoyens canadiens, aux résidents permanents et aux personnes présentes au Canada le droit de demander l'accès aux renseignements personnels que les institutions gouvernementales détiennent à leur sujet, sous réserve d'exemptions et d'exclusions. La Loi établit aussi les règles de transparence en vertu desquelles le gouvernement doit traiter les renseignements personnels. Par exemple, elle exige que les institutions gouvernementales tiennent des fichiers de renseignements personnels décrivant les renseignements personnels qui relèvent d'elles et qui ont été utilisés, sont utilisés ou sont disponibles à des fins administratives. La Loi exige aussi que le président du Conseil du Trésor publie ces fichiers de renseignements personnels, qui sont accessibles au public sur le site Web suivant : https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/acces-information/renseignements-programmes-fonds-renseignements.html.

4.3 La *Loi sur la protection des renseignements personnels* est l'un des éléments du régime global de protection de la vie privée dans le secteur public au Canada. Des règles plus précises peuvent figurer dans d'autres lois et règlements fédéraux selon la fonction gouvernementale – et le type de renseignements. Par exemple, la partie 4 de la *Loi sur le*

ministère de l'Emploi et du Développement social comporte des règles précises au sujet des renseignements personnels servant à l'administration d'importants programmes de soutien social et du revenu, tandis que l'article 241 de la *Loi de l'impôt sur le revenu* restreint le traitement des renseignements concernant les contribuables et que les articles 17 et 18 de la *Loi sur la statistique* restreignent la communication de renseignements recueillis dans le cadre du recensement.

4.4 La *Loi sur la protection des renseignements personnels* constitue également le Commissariat à la protection de la vie privée au Canada. Ombudsman indépendant, le commissaire a le pouvoir de mener des enquêtes sur des plaintes, de formuler des recommandations conformément à la Loi et de présenter des rapports au Parlement. La Loi confère à un individu s'étant vu refuser l'accès, auquel il a droit en vertu de ladite Loi, à ses renseignements personnels le droit de demander à la Cour fédérale de le lui accorder.

4.5 Le commissaire à la protection de la vie privée du Canada reconnaît que, moyennant la conclusion d'un arrangement de représentation approprié avec une personne présente au Canada, tout individu, y compris un non-Canadien à l'extérieur du Canada, peut demander à son agent de présenter une demande d'accès à l'information en vertu de la *Loi sur la protection des renseignements personnels* et autoriser la communication de ses propres renseignements personnels à son agent[5]. La Loi permet également au commissaire de recevoir des plaintes par l'intermédiaire de représentants autorisés et d'enquêter sur ces plaintes et elle habilite lesdits représentants autorisés à exercer le droit à révision judiciaire afférent prévu par la Loi. De plus, « quiconque est directement touché » par la collecte, l'utilisation ou la communication de renseignements personnels peut contester la légalité de l'action du gouvernement par voie de révision judiciaire en vertu de l'article 18.1 de la *Loi sur les Cours fédérales*.

4.6 *Politiques relatives à la « Loi sur la protection des renseignements personnels »* – Le président du Conseil du Trésor du Canada a mis en place plusieurs politiques pangouvernementales qui s'appliquent à l'ensemble des institutions du gouvernement fédéral assujetties à la *Loi sur la protection des renseignements personnels* et qui favorisent l'application de celle-ci à l'échelle du gouvernement. Cela comprend la Politique sur la protection de la vie privée[6], qui établit les exigences d'application de la *Loi sur la protection des renseignements personnels* et de son règlement. Cet instrument de politique est assorti d'une série de directives[7] fixant les exigences liées à la gestion des renseignements personnels, à la réalisation d'évaluations des facteurs relatifs à la vie privée cernant les incidences sur la vie privée des activités ou des programmes nouveaux ou ayant fait l'objet de modifications importantes, aux demandes de renseignements personnels détenus par des institutions fédérales ou de correction de ces renseignements et aux restrictions relatives à l'utilisation du numéro d'assurance sociale ainsi que d'un certain nombre de lignes directrices

---

[5] **Site Web du Commissariat à la protection de la vie privée :** https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/acces-aux-renseignements-personnels/consulter-vos-renseignements-personnels/

[6] **Politique sur la protection de la vie privée :** https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18309

[7] **Directive sur les pratiques relatives à la protection de la vie privée :** https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18309
Directive sur l'évaluation des facteurs relatifs à la vie privée : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308
Directive sur les demandes de renseignements personnels et de correction : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18311
Directive sur le numéro d'assurance sociale : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=13342
Document d'orientation pour aider à préparer des Ententes d'échange de renseignements personnels : https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/protection-renseignement-personnels/document-orientation-aider-preparer-ententes-echange-renseignements-personnels.html
Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché : https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/protection-renseignement-personnels/document-orientation-pris-compte-protection-renseignements-personnels-avant-conclure-marche.html
Lignes directrices sur les atteintes à la vie privée : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26154

ayant trait aux atteintes à la vie privée, aux ententes d'échange de renseignements personnels et aux décisions touchant la passation de marchés.

Réforme de la *Loi sur la protection des renseignements personnels*

4.7 En mars 2016, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (ETHI) a lancé une étude de la *Loi sur la protection des renseignements personnels*. Le 24 novembre 2016, la ministre de la Justice annonçait au Comité ETHI qu'elle dirigeait un examen visant à moderniser la *Loi sur la protection des renseignements personnels* avec l'appui du président du Conseil du Trésor et d'autres collègues. Le ministère de la Justice du Canada dirige ce travail d'examen législatif interministériel, qui prévoit l'examen des recommandations contenues dans le rapport publié par le Comité ETHI le 12 décembre 2016[8].

5.0 La *Charte canadienne des droits et libertés*

5.1 L'article 8 de la *Charte canadienne des droits et libertés* protège le droit à la vie privée, garantissant que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives »[9]. Cette disposition joue dans le cadre juridique canadien un rôle analogue à celui de l'article 7 de la *Charte des droits fondamentaux de l'Union européenne*, de l'article 8 de la *Convention européenne des droits de l'homme* et du Quatrième amendement de la *Constitution des États-Unis*.

5.2 L'article 8 de la *Charte* protège contre les fouilles et perquisitions « abusives »; les tribunaux doivent par conséquent déterminer si une fouille ou perquisition est raisonnable pour savoir si elle enfreint l'article 8. Pour être « raisonnable », une fouille ou perquisition doit être autorisée par la loi, la loi elle-même doit être raisonnable et la fouille ou perquisition doit être effectuée d'une manière raisonnable. Pour être raisonnable, une loi autorisant une violation de la vie privée doit atteindre un juste équilibre entre les intérêts de la société et les droits individuels. Il s'agit d'un critère souple qui peut consister, entre autres, à examiner la nature et de la portée du régime législatif, le mécanisme employé et son éventuel degré d'intrusion, de même que la disponibilité de mesures de supervision judiciaire. Dans le contexte pénal, l'article 8 exige en général d'obtenir un mandat de la cour avant d'effectuer toute fouille ou perquisition. Dans les contextes administratif et réglementaire, la *Charte* est plus souple quant aux pouvoirs de fouille et de perquisition sans mandat.

5.3 En exigeant qu'une fouille ou perquisition soit autorisée par une autorité légitime raisonnable et en permettant aux tribunaux d'invalider des lois déraisonnables et d'ordonner des mesures de redressement en cas d'atteinte déraisonnable à la vie privée, l'article 8 de la *Charte* est un volet important du cadre général de protection de la vie privée au Canada.

5.4 Dans le système juridique canadien, les précédents formant la jurisprudence en matière de droit public sont réputés d'application obligatoire par les tribunaux inférieurs. Par conséquent, le droit découlant de l'article 8 de la *Charte* évolue continuellement au fil des décisions. Suivent de récents exemples de jurisprudence susceptibles d'être pertinents en matière de protection des données des clients; les deux premiers traitent des répercussions sur la vie

[8] Ce rapport est disponible sur le site Web du Comité : http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/rapport-4.

[9] Pour les besoins de l'article 8 de la *Charte*, une « fouille ou perquisition » est toute action de l'État qui viole l'attente raisonnable de protection de la vie privée. L'ensemble des circonstances détermineront s'il y a lieu de s'attendre raisonnablement à la protection de sa vie privée. La protection de l'article 8 s'étend non seulement aux fouilles physiques, mais également aux renseignements personnels.

privée de la fouille d'ordinateurs, tandis que le troisième traite en général de fouilles susceptibles d'être menées à l'insu de leurs sujets.

5.5 En 2013, dans *R. c. Vu*, la Cour suprême du Canada a confirmé qu'un mandat de perquisition visant une résidence ne peut pas implicitement autoriser la fouille de dispositifs électroniques tels qu'un ordinateur découverts sur les lieux. Puisqu'ils peuvent stocker d'immenses quantités de données personnelles, les ordinateurs et appareils semblables ne peuvent faire l'objet d'une fouille que si le juge délivrant le mandat a expressément autorisé celle-ci. Le juge doit donc être persuadé qu'il y a des motifs raisonnables de croire[10] que l'ordinateur visé par la fouille fournira des preuves d'une infraction.

5.6 En 2014, dans *R. c. Spencer*, la Cour suprême du Canada s'est penchée sur la question de savoir si les fournisseurs de services Internet (FSI) pouvaient fournir à la police, en réponse à une demande non contraignante de policiers, l'identité d'un abonné associée à l'utilisation d'une adresse de protocole Internet à un moment particulier. Le tribunal a statué que les attentes raisonnables des internautes quant au respect de leur vie privée comprennent celle de l'anonymat, car une adresse IP peut, lorsqu'elle est associée à une identité, révéler des renseignements de nature très personnelle. Puisque l'abonné dont on voulait obtenir l'identité pouvait raisonnablement s'attendre au respect de sa vie privée, une autorité légitime raisonnable était requise. Le tribunal a statué que le sous-alinéa 7(3)(*c.1*)(ii) de la LPRPDE ne constituait pas une autorité légitime puisqu'elle ne permettait aux organisations de communiquer des données à la police que si celle-ci avait l'autorité légitime de les acquérir. Autrement dit, la police doit s'appuyer sur une source indépendante d'autorité légitime pour obtenir de tels renseignements de FSI.

5.7 Ces dernières années, plus généralement, plusieurs causes ont mis en relief le rôle que peut jouer une révision judiciaire après coup dans l'évaluation du caractère raisonnable d'une loi autorisant une fouille ou perquisition, en particulier dans le cas d'une fouille ou perquisition menée à l'endroit d'une cible qui pourrait autrement ne pas en apprendre la tenue. Par exemple, dans *R. c. Tse*, la Cour suprême du Canada a déterminé que les dispositions du *Code criminel* qui autorisaient la mise sous écoute sans mandat de perquisition en raison de l'urgence de la situation étaient en partie déraisonnables parce qu'elles ne prévoyaient pas de mécanismes visant à prévenir les cibles que leurs communications avaient été interceptées. La notification ayant été jugée nécessaire pour que les cibles de perquisitions puissent contester de telles perquisitions devant les tribunaux, le *Code criminel* a été modifié pour inclure cette exigence. Dans le même ordre d'idées, dans *R. c. Fearon*, la Cour a jugé que la tenue rigoureuse de dossiers était requise pour permettre à une cour de révision d'évaluer correctement la raisonnabilité d'un type particulier de perquisition sans mandat. Voilà quelques exemples de l'approche flexible, décrite ci-dessus, qu'utilisent les tribunaux pour déterminer si une loi autorisant les atteintes à la vie privée est « raisonnable » et, par conséquent, conforme à l'article 8 de la *Charte*.

6.0 Accès à des fins d'application de la loi et de sécurité nationale

Accès à des fins d'application de la loi

6.1 Les principaux outils d'enquête aux fins d'exécution de la loi sont énoncés dans le *Code criminel* du Canada. En font partie les mandats de perquisition, les ordres et ordonnances de préservation, les ordonnances de communication

[10] La norme, reconnue en droit canadien, des « motifs raisonnables de croire » exige qu'une telle croyance repose sur un fondement objectif de renseignements concluants et dignes de foi.

et les autorisations d'écoute électronique. Des pouvoirs d'enquête aux fins d'application de la loi sont aussi décrits dans la *Loi sur l'entraide juridique en matière criminelle* (LEJMC), qui autorise le Canada à aider des partenaires étrangers à obtenir des preuves et à leur offrir d'autres formes d'assistance pour la tenue d'enquêtes pénales et de poursuites au criminel. En vertu de la LEJMC, le Canada peut obtenir des ordonnances d'un tribunal au nom de partenaires étrangers, y compris des mandats de perquisition, d'autres mandats, des ordonnances de communication et des assignations à témoigner.

6.2 Le niveau d'autorisation judiciaire préalable requis par une autorité pour utiliser certaines techniques d'enquête témoigne et dépend du degré d'intrusion de la technique en question et de l'attente raisonnable d'un individu de ne pas voir cette technique violer sa vie privée.

6.3 *Autorisation judiciaire préalable* – Les techniques d'enquête qui permettent à la police et à d'autres organismes d'application de la loi d'obtenir des renseignements par voie de perquisition et de saisie exigent en général une autorisation judiciaire préalable si l'on peut raisonnablement s'attendre au respect de sa vie privée, bien qu'il y ait ces exceptions à cette règle générale, comme les situations d'urgence. La demande d'autorisation préalable est habituellement entendue ex parte, ce qui signifie que le suspect n'est pas représenté puisque sa participation à cette étape de l'enquête nuirait à la capacité de la police de recueillir des éléments de preuve et révélerait des techniques d'enquête délicates.

6.4 Deux normes judiciaires sont d'usage courant dans le *Code criminel* du Canada : les motifs raisonnables de croire – dans le cas de renseignements ou techniques assorties d'une attente plus élevée de la personne quant au respect de sa vie privée – et les motifs raisonnables de soupçonner – dans le cas de renseignements assortis d'une attente moindre de la personne quant au respect de sa vie privée (p. ex. les numéros de téléphone composés) et de techniques d'enquête moins intrusives. En droit canadien, les motifs raisonnables de croire, ou de soupçonner, sont une norme reconnue devant se fonder objectivement sur des renseignements concluants et dignes de foi.

6.5 *Mandats et ordres* – Bien que le *Code criminel* prévoie un éventail de processus judiciaires, ceux concernant les techniques d'enquête se divisent généralement en deux catégories : les mandats et les autorisations, qui autorisent des acteurs étatiques tels que les agents d'application de la loi à faire quelque chose; et les ordonnances, qui obligent les civils à faire quelque chose.

6.6 Les mandats et les autorisations autorisent généralement la police à faire quelque chose qui aurait une incidence sur l'attente raisonnable d'une personne quant au respect de sa vie privée. Par exemple, un mandat de perquisition autorise la police à pénétrer dans un local pour y trouver des preuves d'une infraction. Les ordonnances de communication, en revanche, contraignent un tiers à compiler des documents ou des données en sa possession ou sous son contrôle pour les besoins de l'enquête.

6.7 *Mandat de perquisition* – Le mandat de perquisition est un outil qu'utilise la police afin de procéder à une fouille, par exemple d'un domicile, d'un ordinateur ou d'une voiture. Étant assorti d'un vaste pouvoir, le mandat de perquisition n'est accordé qu'une fois atteint le critère des motifs raisonnables de croire.

6.8 *Mandat de localisation* – Le mandat de localisation permet de localiser le lieu où se trouvent des opérations (p. ex. les relevés de carte de crédit), le lieu ou les déplacements d'une chose (p. ex. un véhicule) ou les déplacements d'une personne physique par l'identification du lieu d'une chose qu'elle a l'habitude de porter ou transporter (p. ex. un

téléphone cellulaire). Les mandats de localisation ont été mis à jour dans la *Loi sur la protection des Canadiens contre la cybercriminalité*, qui est entrée en vigueur en mars 2015, pour tenir compte des avancées technologiques, en particulier la précision de tels dispositifs et leur potentiel d'incidence accrue sur la vie privée, en augmentant le degré de contrôle judiciaire requis lorsque ces mandats servent à localiser des personnes à l'aide d'une chose qu'elles ont l'habitude de porter ou de transporter.

6.9 *Mandat pour un enregistreur de données de transmission* – Le nouveau mandat pour un enregistreur de données de transmission[11], qui a pris effet avec la *Loi sur la protection des Canadiens contre la cybercriminalité*, a remplacé l'ancien mandat pour enregistreur de numéro afin d'étendre l'application de la technique d'enquête aux télécommunications par Internet.

6.10 *Autorisation d'écoute électronique* – Depuis 1974, il s'agit d'une infraction au Canada que d'intercepter une communication privée d'autrui à moins d'y être autorisé en vertu du *Code criminel*. La partie VI du *Code criminel* établit un certain nombre de méthodes permettant d'autoriser la police à intercepter les communications privées de Canadiens, dont le contenu de communications, y compris par autorisation judiciaire préalable et en situation d'urgence.

6.11 *Mandat général* – L'on peut obtenir un mandat général pour utiliser des techniques d'enquête ne figurant dans aucun autre mandat du *Code criminel*. Le mandat général peut être utile à la police lorsqu'elle souhaite obtenir une autorisation judiciaire préalable pour des situations uniques ou inusitées ou dans le cas d'environnements nouveaux ou en évolution.

6.12 *Ordonnance d'assistance* – À l'appui d'un mandat ou d'une autorisation, un juge peut aussi rendre une ordonnance d'assistance obligeant un tiers à prêter toute assistance dont on peut raisonnablement conclure à la nécessité pour donner effet au mandat ou à l'autorisation.

6.13 *Préservation des données*[12] – Des outils de préservation des données ont été introduits dans le *Code criminel* par la *Loi sur la protection des Canadiens contre la cybercriminalité*. Ces outils empêchent la suppression des données informatiques jusqu'à ce que la cour autorise la délivrance d'une ordonnance ou d'un mandat pour les acquérir.

6.14 *Ordonnances de communication* – Les ordonnances de communication vont d'ordonnances pouvant obliger à communiquer des données et documents assortis d'une attente plus élevée quant au respect de sa vie privée à des ordonnances visant la communication de renseignements plus précis, moins personnels et limités. Le *Code criminel* prévoit des ordonnances de communication depuis 2004, mais la *Loi sur la protection des Canadiens contre la cybercriminalité* en a ajouté trois à seuil juridique moindre pour aider la police en début d'enquête. Ces nouvelles ordonnances de communication à seuil inférieur donnent à la police des outils qui leur permettent de recueillir des données de transmission, des données de localisation et des données de retraçage et s'ajoutent à l'ordonnance, existante, de communication à seuil juridique moindre de données financières de base. Si les données ou les

[11] Une donnée de transmission s'entend de toute donnée relative à la transmission d'une télécommunication. Toutefois, cette définition demeure aussi restreinte que la précédente puisqu'elle exclut le contenu de la communication, n'incluant que l'information sur le mode de transmission de la communication de l'expéditeur au destinataire.

[12] Au Canada, le terme « préservation des données » n'est pas synonyme de « stockage de données » et renvoie à l'obligation générale faite aux fournisseurs de services de recueillir et de stocker certaines données pendant une période prescrite pour l'ensemble des abonnés, qu'ils fassent l'objet ou non d'une enquête. Le stockage général des données n'est pas une exigence au Canada.

renseignements que permettent d'obtenir ces ordonnances de communication à seuil inférieur sont de nature personnelle, il ne s'agit toutefois pas d'information très privée ou révélatrice.

6.15 La *Loi sur la protection des Canadiens contre la cybercriminalité* a également modifié la LEJMC en y intégrant les nouvelles ordonnances de communication du *Code criminel* qui permettent de recueillir des données à un seuil juridique moindre. La modification a également créé un régime procédural distinct pour l'exécution des ordonnances de localisation et les ordonnances de communication de données de transmission prévues au *Code criminel*. Elle simplifie également le processus d'envoi du fruit des nouvelles ordonnances de communication et des nouveaux mandats au partenaire étranger. Ces pouvoirs sont un élément essentiel de la nouvelle trousse d'outils d'application de la loi du Canada. L'incapacité du Canada d'aider ses partenaires étrangers à réaliser ses enquêtes l'empêcherait à son tour de solliciter leur aide pour obtenir des preuves numériques et de participer pleinement à la lutte mondiale contre les formes graves de criminalité internationale.

Accès à des fins de sécurité nationale

6.16 Le Service canadien du renseignement de sécurité (SCRS), le service intérieur de renseignement de sécurité du Canada, a pour rôle d'enquêter sur les activités soupçonnées de menacer la sécurité du Canada et d'en rendre compte au gouvernement du Canada. Ses activités sont régies par la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS), qui comporte des exigences en matière de collecte, d'utilisation, de conservation et de communication de renseignements. Le SCRS doit également mener ses activités conformément à la *Loi sur la protection des renseignements personnels* et à la *Charte canadienne des droits et libertés*.

6.17 *Autorisation judiciaire préalable* – Le SCRS doit obtenir l'autorisation judiciaire préalable d'utiliser des techniques d'enquête dans le cas d'individus pouvant raisonnablement s'attendre au respect de leur vie privée en vertu de l'article 8 de la *Charte*. La demande d'autorisation préalable est entendue ex parte, ce qui signifie que le sujet de l'enquête n'est pas représenté. Le faire participer porterait atteinte à la sécurité nationale du Canada en révélant des techniques d'enquête délicates.

6.18 La norme judiciaire des « motifs raisonnables de croire » et d'autres conditions doivent être respectées avant qu'un juge ne délivre un mandat en vertu de la Loi sur le SCRS. Le dossier qui lui est présenté sous serment par le directeur ou un employé désigné à cette fin doit convaincre le juge que, entre autres choses : 1) le mandat est requis pour faire enquête sur une menace à la sécurité du Canada (au sens de l'article 2 de la Loi sur le SCRS[13]); 2) d'autres méthodes d'enquête ont été essayées en vain ou semblent avoir peu de chances de succès; et 3) l'urgence de l'affaire est telle qu'il serait très difficile de mener l'enquête en ne recourant qu'à d'autres techniques d'enquête ou il est probable que, sans mandat, des informations importantes concernant la sécurité du Canada ou l'exécution du mandat du SCRS de recueillir, au Canada, du renseignement étranger, ne pourraient être acquises.

6.19 Plusieurs autres exigences de la Loi sur le SCRS encadrent les activités du SCRS. Par exemple, le SCRS doit obtenir l'approbation du ministre de la Sécurité publique et de la Protection civile avant de demander un mandat à la Cour fédérale. Le ministre donne aussi des instructions quant aux procédures opérationnelles à suivre et approuve les ententes de coopération conclues et les relations établies avec des services de renseignement étrangers. La Loi sur le

[13] Le SCRS peut aussi, conformément à l'article 16 de la Loi sur le SCRS, recueillir du renseignement étranger au Canada. Cela représente toutefois un volet étroit du mandat du SCRS, lequel consiste surtout à faire enquête sur des activités soupçonnées de menacer la sécurité du Canada (en vertu de l'article 12) et de mener des enquêtes pour fournir des évaluations de sécurité et des conseils (articles 13, 14 et 15).

SCRS prévoit également un rigoureux système d'examen par le Comité de surveillance des activités de renseignement de sécurité (CSARS), qui a accès à toute information détenue par le SCRS. Le CSARS a pour mandat de rendre annuellement compte au Parlement du Canada des activités du SCRS.

6.20 La *Loi sur le recyclage des produits de la criminalité* a été modifiée en décembre 2001, devenant la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* (LRPCFAT), laquelle a pour objet :

- « de mettre en œuvre des mesures[14] visant à détecter et décourager le recyclage des produits de la criminalité et le financement des activités terroristes et à faciliter les enquêtes et les poursuites relatives aux infractions de recyclage des produits de la criminalité et aux infractions de financement des activités »;
- « de combattre le crime organisé en fournissant aux responsables de l'application de la loi les renseignements leur permettant de priver les criminels du produit de leurs activités illicites, tout en assurant la mise en place des garanties nécessaires à la protection de la vie privée des personnes à l'égard des renseignements personnels les concernant »;
- « d'aider le Canada à remplir ses engagements internationaux dans la lutte contre le crime transnational, particulièrement le recyclage des produits de la criminalité, et la lutte contre les activités terroristes ».

6.21 En 2014, la LRPCFAT a de nouveau été modifiée afin : d'accroître les obligations des institutions financières et des intermédiaires financiers en ce qui touche la vérification de l'identité des clients, la tenue de documents et l'inscription, de mentionner les casinos en ligne et d'étendre son application aux personnes et aux entités qui se livrent au commerce de la monnaie virtuelle et aux entreprises de services monétaires étrangères. Des modifications ont aussi été apportées aux renseignements que le CANAFE peut recevoir, recueillir ou divulguer et pour étendre les circonstances dans lesquelles le CANAFE ou l'Agence des services frontaliers du Canada peut divulguer des renseignements reçus ou recueillis en vertu de la Loi. Le projet de loi afférent a également mis à jour les dispositions de révision et d'appel relatives au programme de déclaration des mouvements transfrontaliers des devises et a mis en vigueur la partie 1.1 de la Loi.

7.0 Évolutions récentes

7.1 Consultation sur la sécurité nationale

Lorsque l'ancien projet de loi C-51, la *Loi antiterroriste* (ATA), a été déposé à la Chambre des communes, nombreux ont été les Canadiens à se demander si la loi proposée permettrait de protéger adéquatement la sécurité et les droits. Ces préoccupations n'ayant pas décru depuis l'adoption de la *Loi antiterroriste* en 2015, le premier ministre du Canada a chargé le ministre de la Sécurité publique et de la Protection civile, par voie de lettre de mandat, de mener à bien des priorités parmi lesquelles figurent :

- « créer un comité statutaire composé de parlementaires ayant un accès spécial à l'information classifiée pour examiner les ministères et les agences qui ont des responsabilités en matière de sécurité nationale », et

[14] Les mesures comprennent : imposer des obligations de tenue de documents et d'identification des clients aux fournisseurs de services financiers et autres personnes ou entités; établir un régime de déclaration obligatoire des opérations financières douteuses et des mouvements transfrontaliers d'espèces et d'effets; et constituer un organisme (Centre d'analyse des opérations et déclarations financières du Canada) chargé de l'examen de renseignements, notamment ceux portés à son attention.

- « travailler à la révocation des éléments problématiques du projet de loi C-51 et adopter de nouvelles mesures législatives renforçant la reddition de compte en matière de sécurité nationale et mieux équilibrer la sécurité collective avec les droits et les libertés ».

7.2 Tout en travaillant à la réalisation des engagements découlant de ce mandat, le gouvernement a consulté la population canadienne sur les grands éléments des lois et politiques de sécurité nationale du Canada pour veiller à ce que celles-ci protègent efficacement la sécurité des Canadiens et reflètent également leurs droits, valeurs et libertés. La consultation s'appuyait sur *Notre sécurité, nos droits : livre vert sur la sécurité nationale de 2016* et sur un document de contexte détaillé donnant ensemble un aperçu de dix grandes questions de sécurité nationale[15]. Cette consultation s'est déroulée de septembre à décembre 2016 et s'est traduite par l'obtention de réponses en ligne à un questionnaire, la présentation de propositions par courriel, la tenue d'assemblées publiques et d'activités en ligne, la participation d'intervenants et d'universitaires clés et la réalisation d'examens par des comités parlementaires.

7.3 Dans le cadre de cette consultation, le gouvernement a entendu des témoignages d'experts, d'universitaires, de responsables de la sécurité et du renseignement, de parlementaires et sénateurs, de groupes de la société civile et de Canadiens. Près de 60 000 réponses au questionnaire en ligne et plus de 17 000 réponses par courriel ont été reçues. Un rapport à diffusion publique sur les résultats de la consultation est en voie de préparation et des sommaires des assemblées publiques sont disponibles[16]. Le gouvernement rend les propositions qu'il a reçues en ligne et par courriel accessibles dans son portail « Gouvernement ouvert ».

7.4 Le gouvernement continue d'analyser l'information et l'utilisera afin d'élaborer les futures politiques de sécurité nationale du Canada et d'apporter des modifications aux lois et programmes en meilleure connaissance de cause, l'objectif étant d'assurer l'efficacité des outils mis à la disposition des organismes d'application de la loi et de sécurité tout en protégeant les droits et libertés des Canadiens. Le ministre de la Sécurité publique et de la Protection civile a déclaré publiquement son intention de déposer les modifications proposées à l'ancien projet de loi C-51.

7.5 *Loi sur la communication d'information ayant trait à la sécurité du Canada*

La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) a été promulguée en 2015 dans le cadre de la *Loi antiterroriste*. Elle permet expressément à l'ensemble des institutions fédérales de communiquer, à leur discrétion, des renseignements personnels à un nombre limité d'institutions fédérales qui sont désignées destinataires des renseignements au titre de la LCISC sur la base de leur compétence ou de leurs responsabilités en matière de sécurité nationale, à condition que les renseignements soient pertinents aux fins de l'exercice de cette compétence ou de ces responsabilités. En vertu de la LCISC, les renseignements doivent être communiqués au responsable d'une institution destinataire ou aux délégués de celle-ci.

7.6 La LCISC n'a ni pour effet de remplacer les pouvoirs existants en matière de communication d'information ni pour effet d'y porter atteinte. D'autres limites réglementaires à la communication et à la collecte de renseignements de même qu'à la gestion générale de l'information s'appliquent aux renseignements communiqués en vertu de la LCISC.

[15] Les dix principales questions de sécurité nationale sont : la responsabilisation; la prévention; la réduction de la menace; la communication interne d'information sur la sécurité nationale; le Programme de protection des passagers; les mesures de lutte contre le terrorisme prévues au *Code criminel*; les procédures d'inscription à la liste des entités antiterroristes; le financement terroriste; les capacités d'enquête dans le monde numérique; et le renseignement et la preuve. Voir https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-fr.aspx#s9.

[16] Pour les sommaires des assemblées publiques, prière de consulter https://www.canada.ca/fr/services/defense/securitenationale/consultation-securite-nationale.html.

Par exemple, les exigences prévues à la *Loi sur la protection des renseignements personnels* continuent de s'appliquer aux renseignements personnels communiqués aux termes de la LCISC.

7.7 *Loi sur la sûreté des déplacements aériens*, 2015

En août 2015, la *Loi sur la sûreté des déplacements aériens* (LSDA) est entrée en vigueur, élargissant le mandat du Programme de protection des passagers pour permettre au ministre de la Sécurité publique et de la Protection civile d'établir une liste d'individus (la liste établie en vertu de la LSDA) dont il y a des motifs raisonnables de soupçonner qu'ils participeront ou tenteront de participer à un acte qui menacerait la sûreté des transports ou de se déplacer en aéronef dans le but de commettre certaines infractions de terrorisme.

7.8 De plus, la LSDA permet au ministre de conclure des ententes écrites pour communiquer, en tout ou en partie, la liste établie en vertu de la LSDA à des partenaires étrangers. Il s'agit d'ententes administratives qui ne lient juridiquement ni l'une ni l'autre partie. L'information est communiquée conformément au droit canadien et fait l'objet de mesures de protection afin de protéger la vie privée et de restreindre son utilisation et sa communication ultérieures.

8.0 Renseignements complémentaires et rapports

8.1 Pour de plus amples renseignements sur tout aspect du présent rapport, prière de s'adresser à Charles Taillefer, directeur, Direction de la politique sur la vie privée et la protection des données, Direction générale des politiques numériques, Innovation, Science et Développement économique Canada, 235, rue Queen, 1er étage, Ottawa (Ontario), Canada K1A 0H5 (Charles.Taillefer@Canada.ca).

8.2 Les prochains rapports devraient paraître à intervalle régulier. Le présent rapport étant le premier, le gouvernement sera heureux de tout commentaire sur sa présentation et son utilité. Les prochains devraient être beaucoup plus courts compte tenu de la période à l'étude dans celui-ci.